



# DELTA RISK

CYBER SECURITY | BUSINESS RESILIENCY | RISK MANAGEMENT



## CYBER EXERCISE

ACHIEVING VALUE THROUGH INNOVATIVE DESIGN BEST-PRACTICES

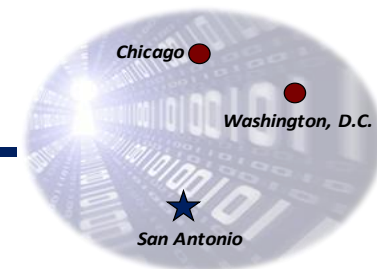
Presented to  
6<sup>th</sup> Annual GFIRST National Conference

San Antonio, Texas

17 July 2010

Chris Fogle, CISSP

Delta Risk, LLC



- Cyber security & risk management group
- Public-private partnerships in Cyber and Homeland Security
- Principals with 50+ years experience in National Security-
  - cyber warfare, tactics, and training*
  - Planning and execution of DOD/national cyber defense exercises
  - BLACK DEMON, DARK SCREEN, Livewire, Cyber Storm, BULWARK DEFENDER

- Experience in large enterprise network security & defense, and business continuity
  - Focus on “demonstrated response” vs. “documented compliance”
  - Design and execute cyber defense training and assessment events against realistic threats

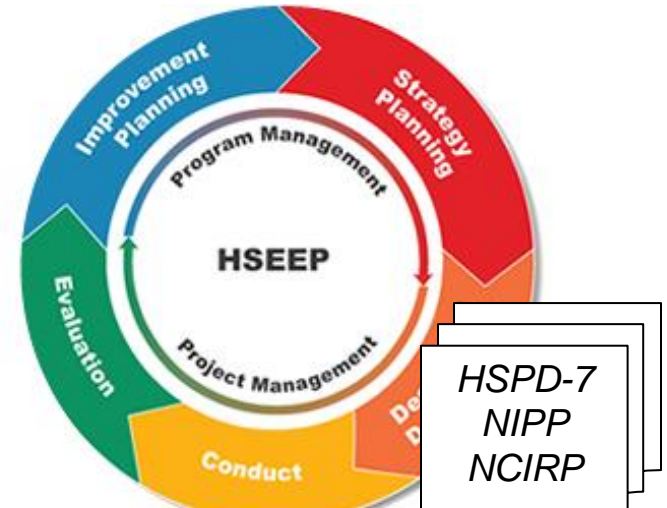
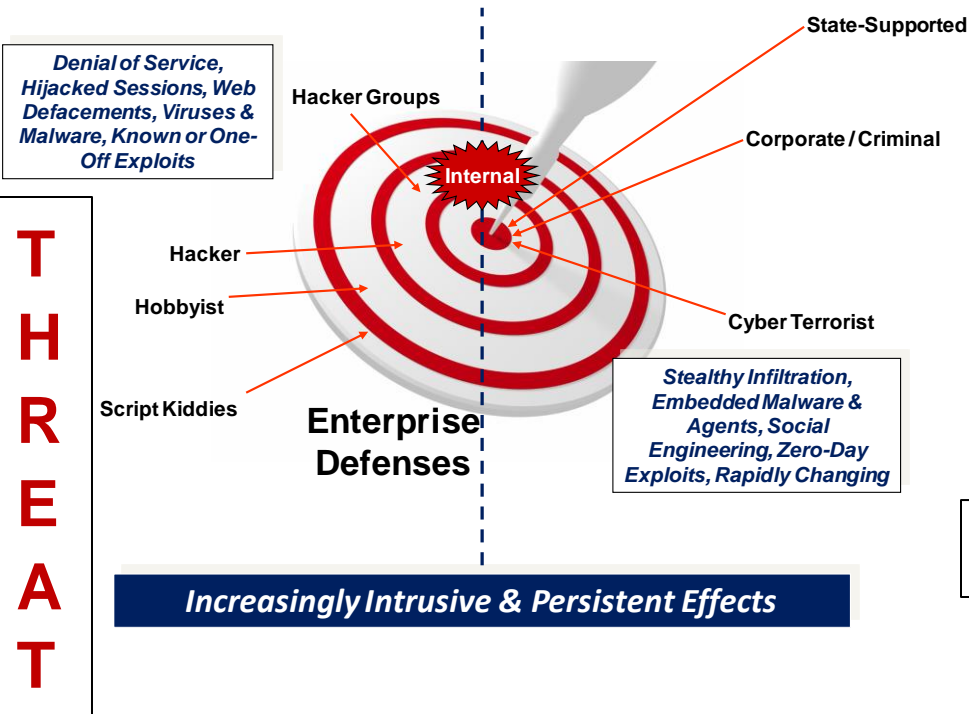


# Overview

---

- Cyber exercises are increasingly important tools for training, assessing, and sharing information
- State of the Art not where it could be; need to “raise the bar”
- Better (more advanced, more value-added) cyber exercises are possible with a little creativity and some evolving technologies

# Relevant landscape for cyber exercises...



## PROGRAMS & DIRECTIVES

... increasing attention  
... recognized value



---

...what we mean by “Advanced Cyber Exercise”

# CONTEXT

# What is an “Exercise”...?

## Evaluation

- *Standardization*
- *People & Positions*

## Test

- *New procedures*
- *Technologies*

## Assessment

- *Discover vulnerabilities*
- *Defenses (capacity & metrics)*

## Drill

- *Training & Practice*

---

## Exercise

More accurate than talking about it ... when it's done right  
More realistic training for your staff  
Best test of combined people, processes, and technology

# What is a “Cyber Exercise”...?

- Cyberspace
  - Interdependent domain ... information infrastructures ... Internet, telecommunications, computers, and embedded systems
- Cyber Attack
  - Attack ... targeting enterprise's use of cyberspace ... disrupting, disabling, destroying, or maliciously controlling ... infrastructure, data, information, operations
- Cyber Incident
  - Actions through networks that result in ... adverse affect on information system or information therein

*Adapted from: Committee on National Security Systems (CNSS)  
Instruction 4009, National Information Assurance (IA) Glossary, 26 Apr  
2010*

**Cyber Exercise ... objectives focus on protecting,  
defending, and recovering cyber assets and operations  
from a cyber attack or cyber incident**

# HSEEP handles the science of exercises fairly well

- Defined formats, documentation, and processes
- Correctly focused on improvement planning
- Rich history of success in *physical* domains
- Fairly robust formal program



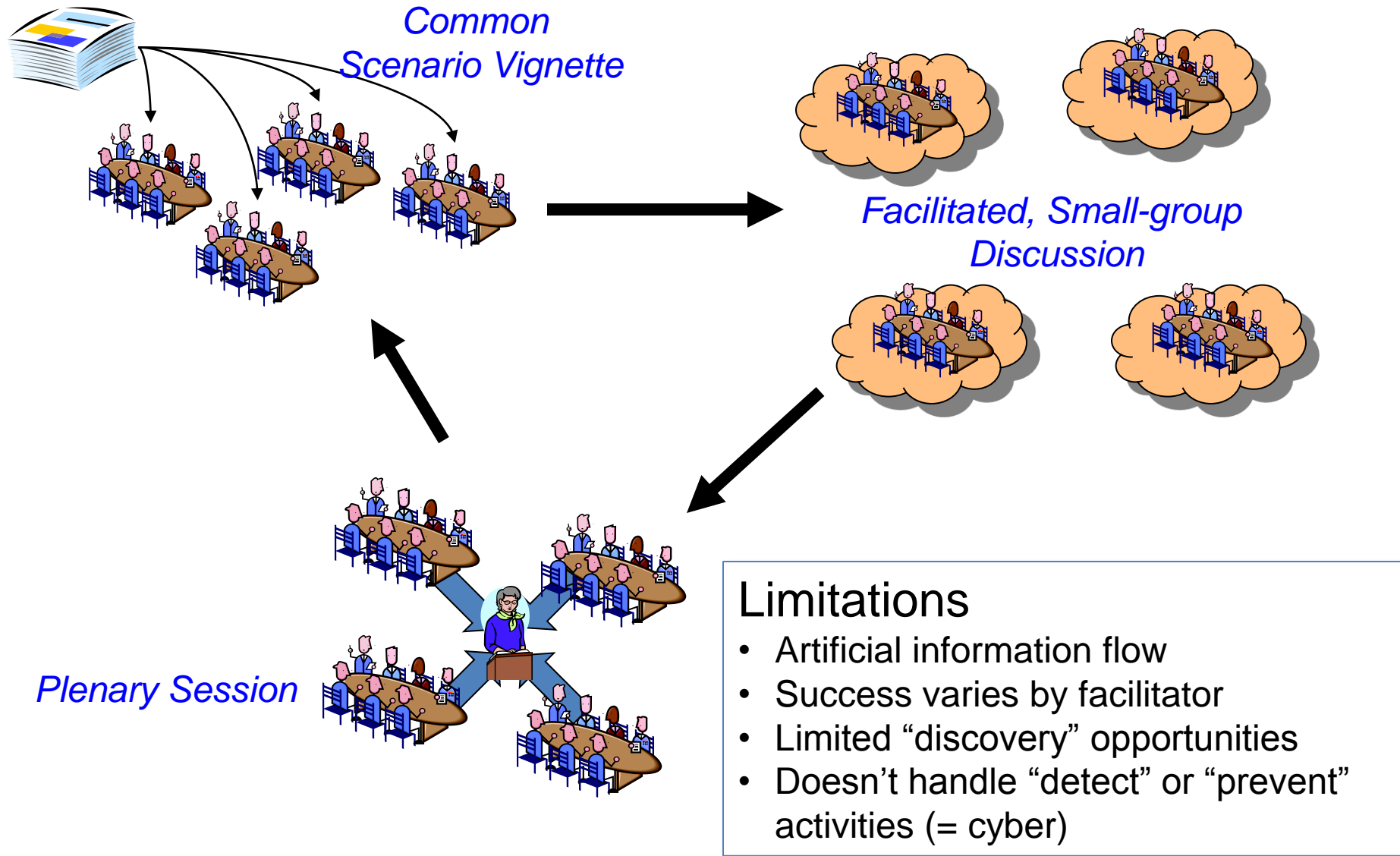
*... so why talk about it?*

*Seminar  
Workshop  
TTX  
Game*

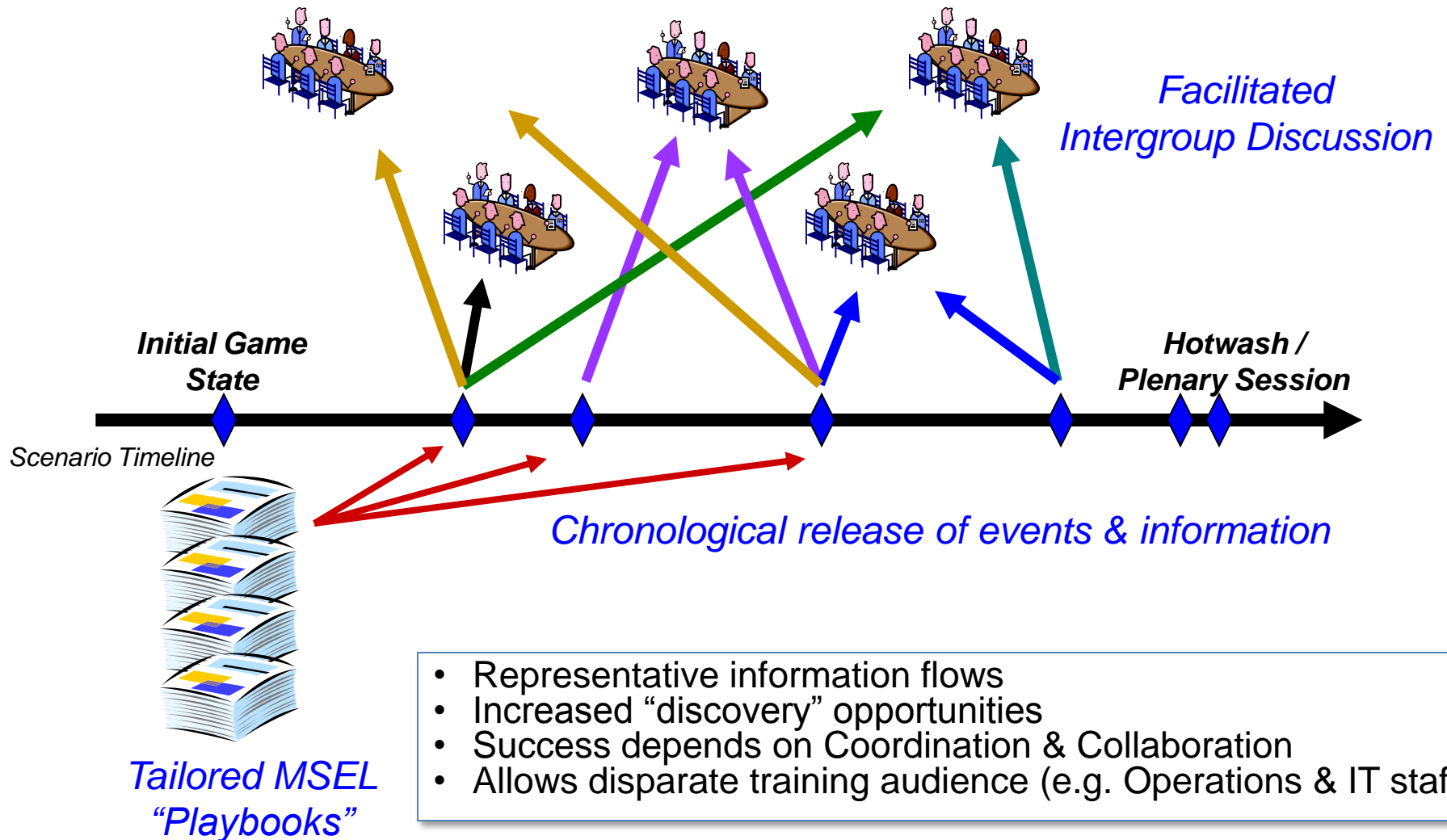
*Drill  
Functional Exercise  
Full-Scale Exercise*



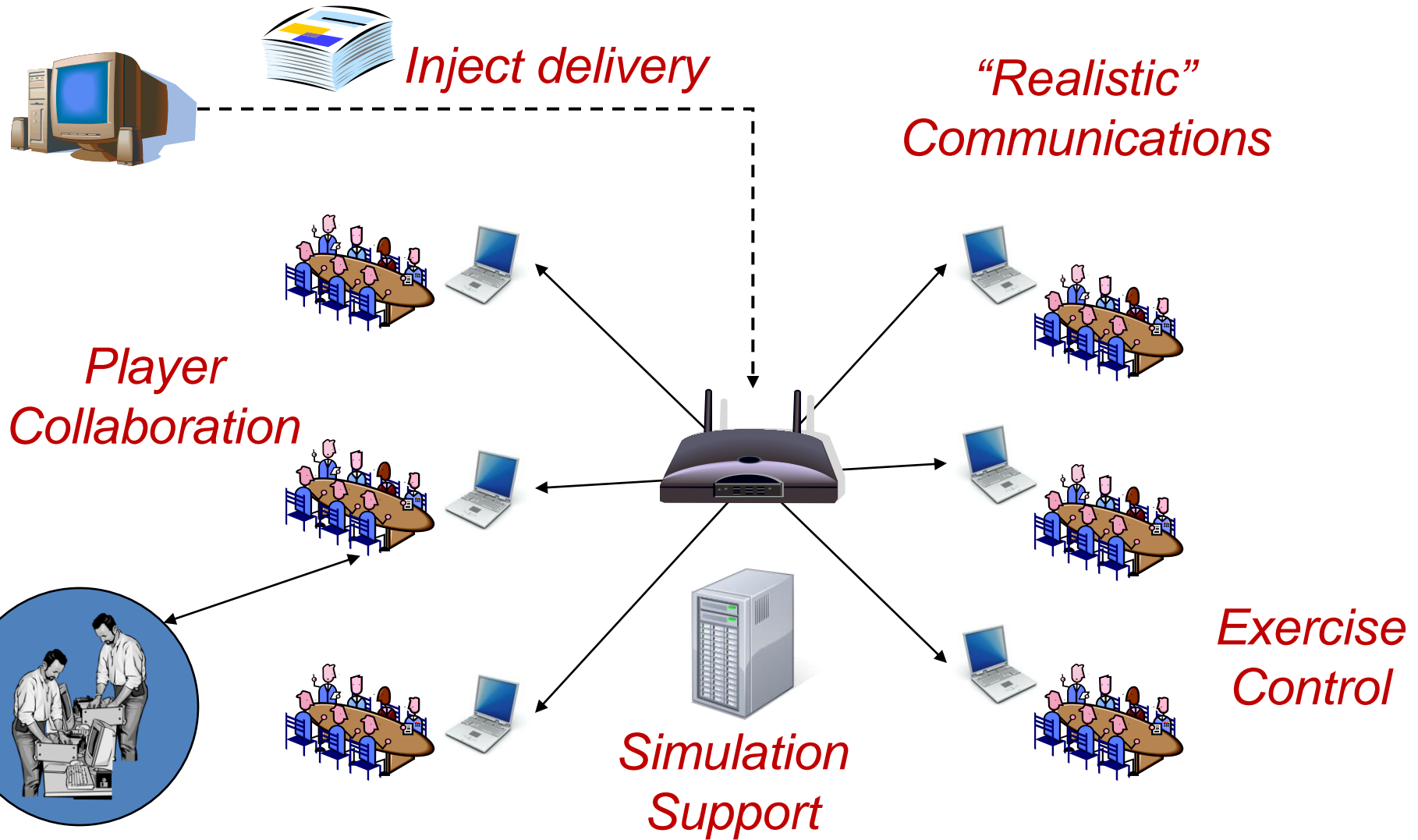
# Typical Tabletop (cyber) Exercise



# Advanced Tabletop Format



# System Extensions / Options



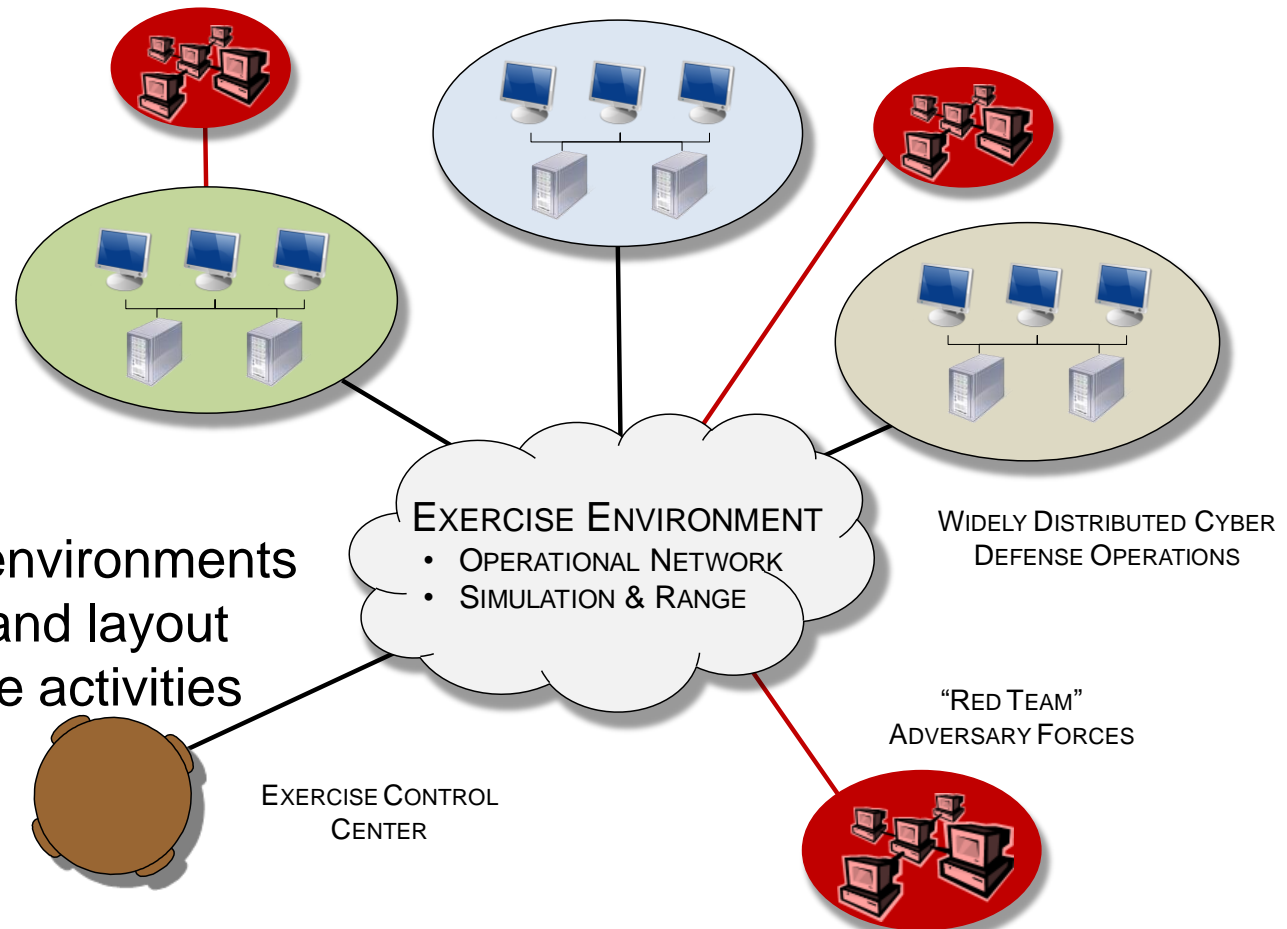
# What is an “Advanced Cyber Exercise”...?

- Relevant models
  - HSEEP-defined *Full-Scale Event*
  - *BLACK DEMON*



## Attributes

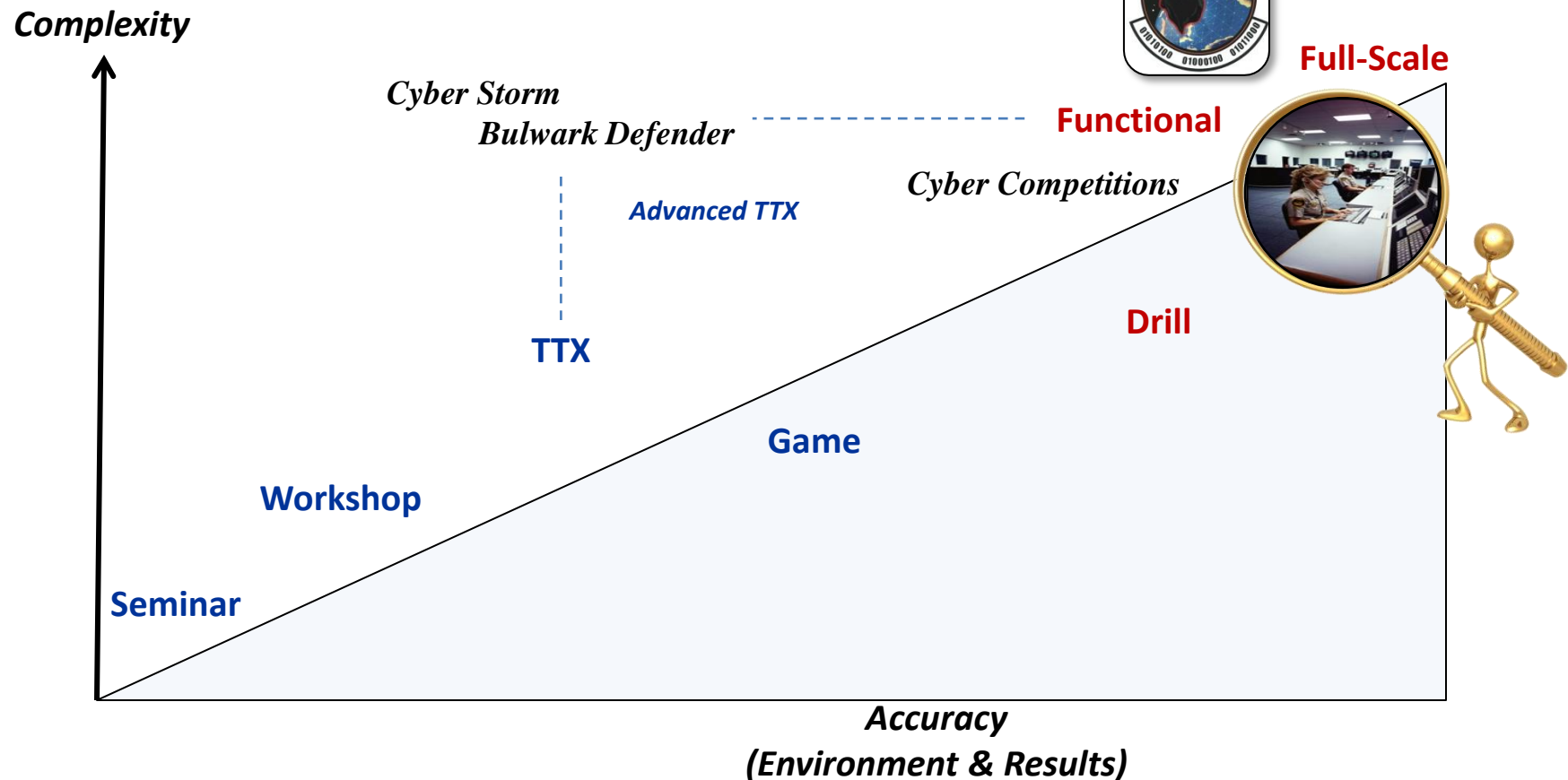
- Hands-on, technical
- Threat emulation
- Realistic operating environments
  - Same systems and layout
- Spans cyber defense activities



# Current State of Play

## Assessment:

- Private Sector gaining experience in formal exercise processes
- *Necessity* and *Invention* beginning to intersect
- ...but, State of the Art not where it could be; need to “raise the bar”



---

...how do we raise the bar?

## **METHODS & PRACTICES**

# **THE “ART” OF EXERCISES**

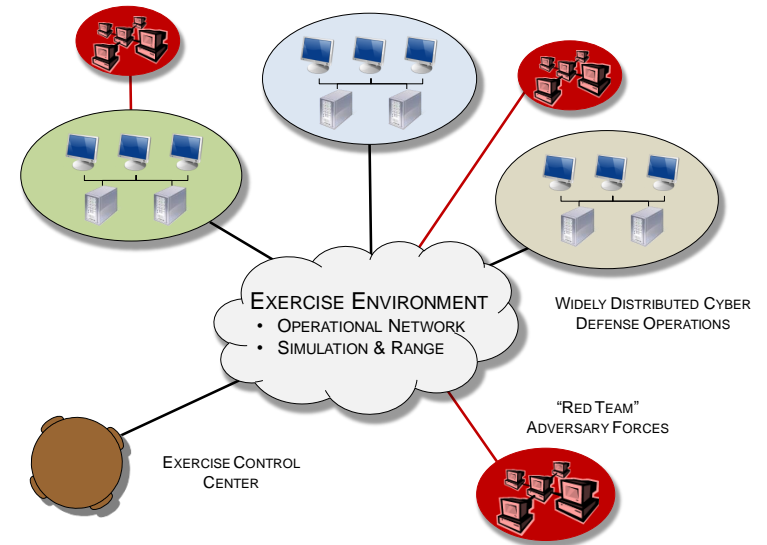
# Raising the Bar

... means identifying and developing methods and practices that will:

- Increase Realism
- Manage Complexity
- Foster Repeatability

## Innovation in:

- Scenario planning
- Operational networks and live-action aggressors
- Simulators and Ranges



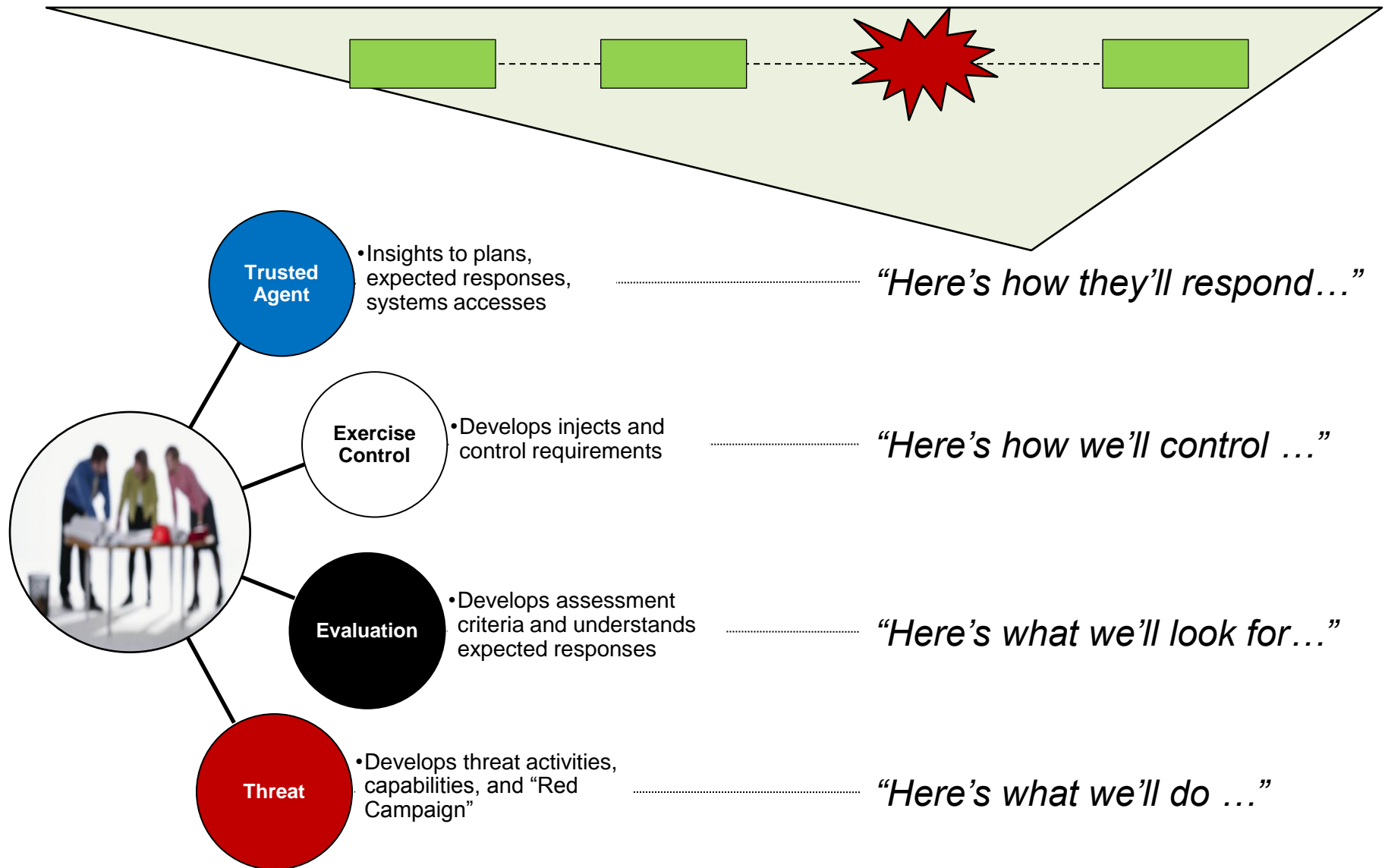
---

... the time in an exercise when the MOST learning takes place

## **SCENARIO DEVELOPMENT & PLANNING**



# Scenario Planning Team



# Scenario Planning

*“What kind of scenario should we have?”*

Effect

“I want to disrupt public access to my online services”

Threat

“I want to see a botnet attack scenario”

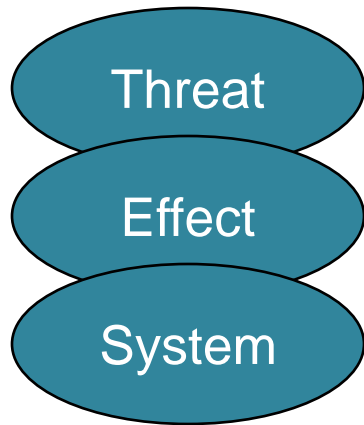
System

“I want an attack against the vehicle registration system”



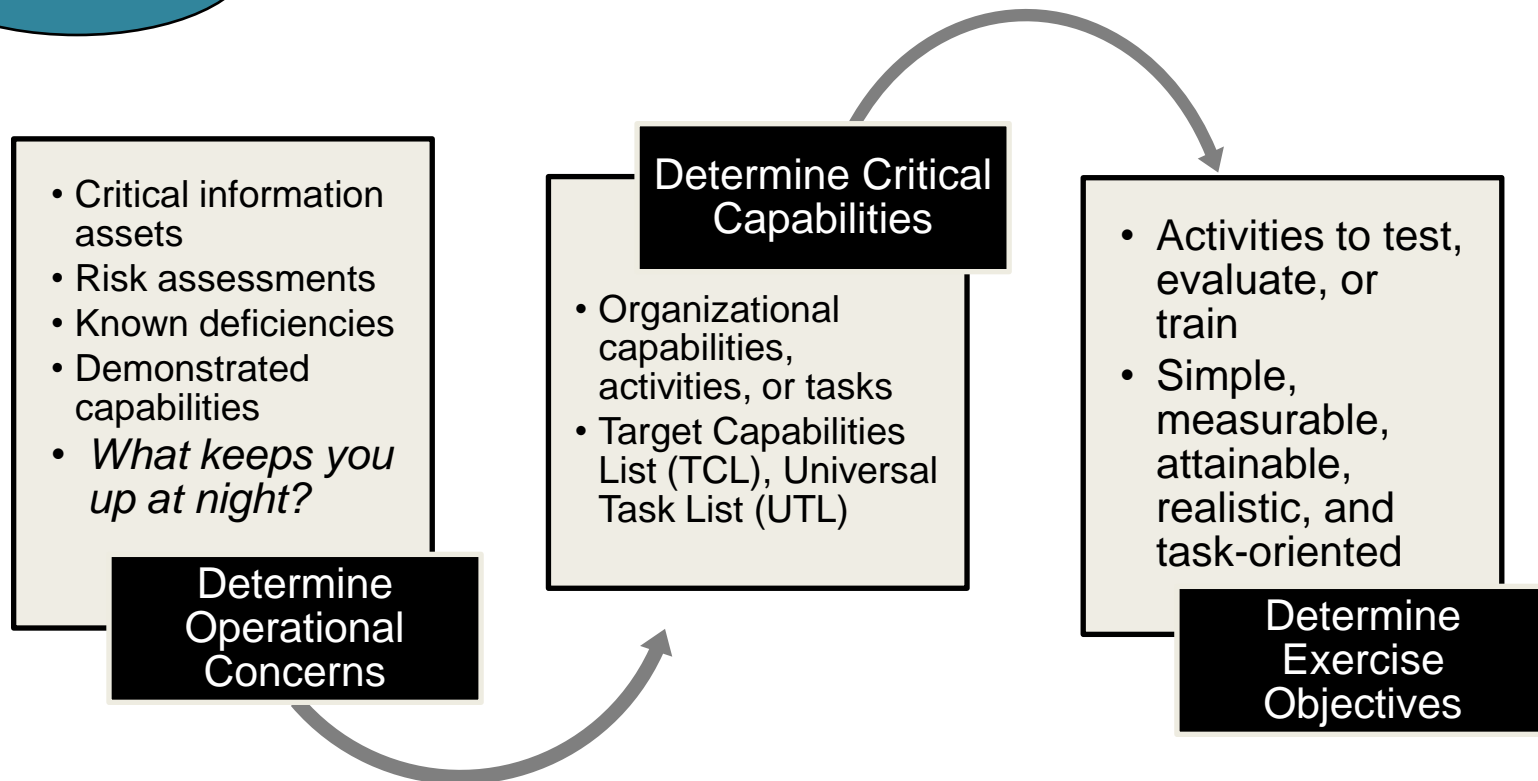
*... you must be ready to accommodate all three perspectives.*

# Scenario Planning

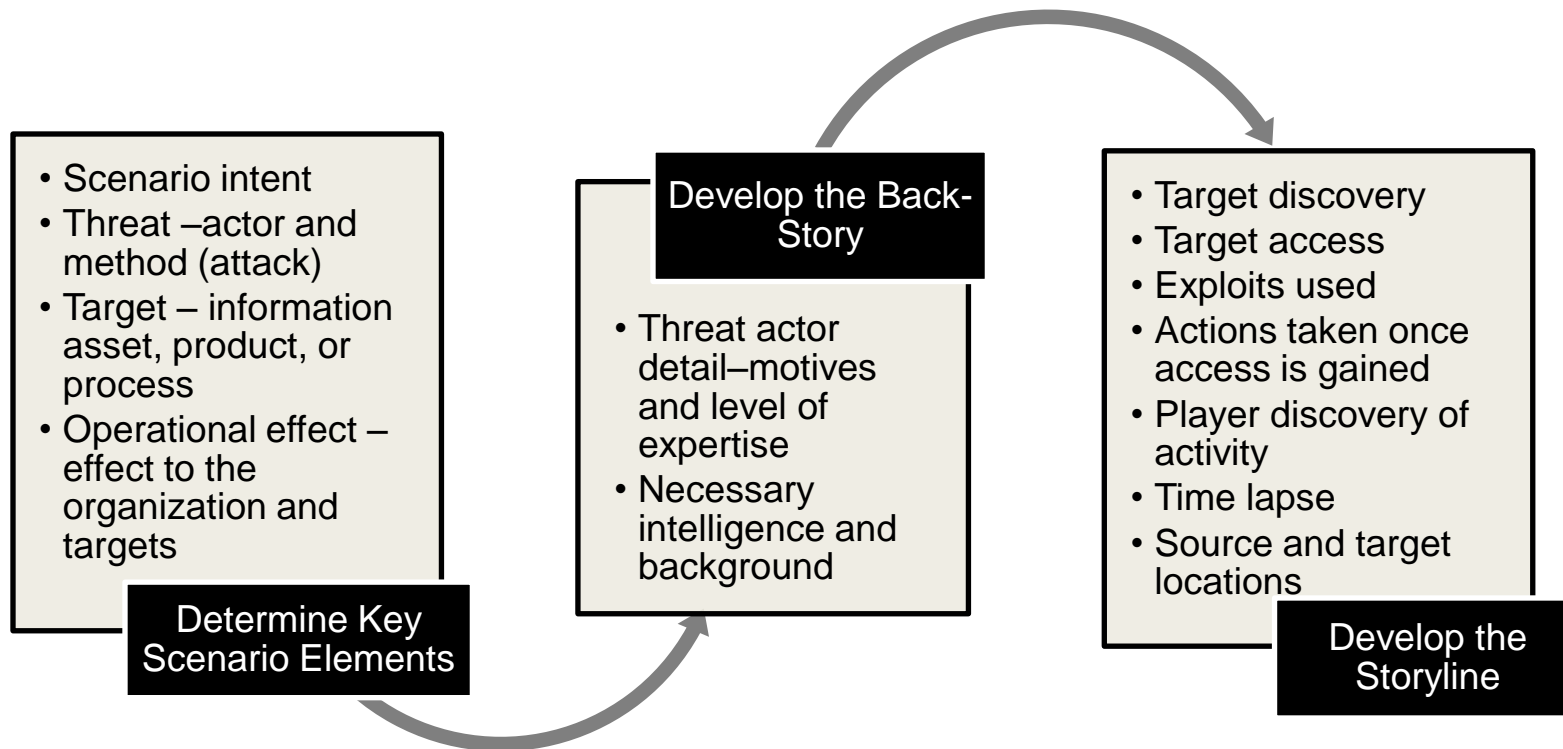


## Consider

- Your incidents (“*First-hand Knowledge*”)
- Publicly reported activities (“*Researched*”)
- Creatively developed events (“*What If...*”)



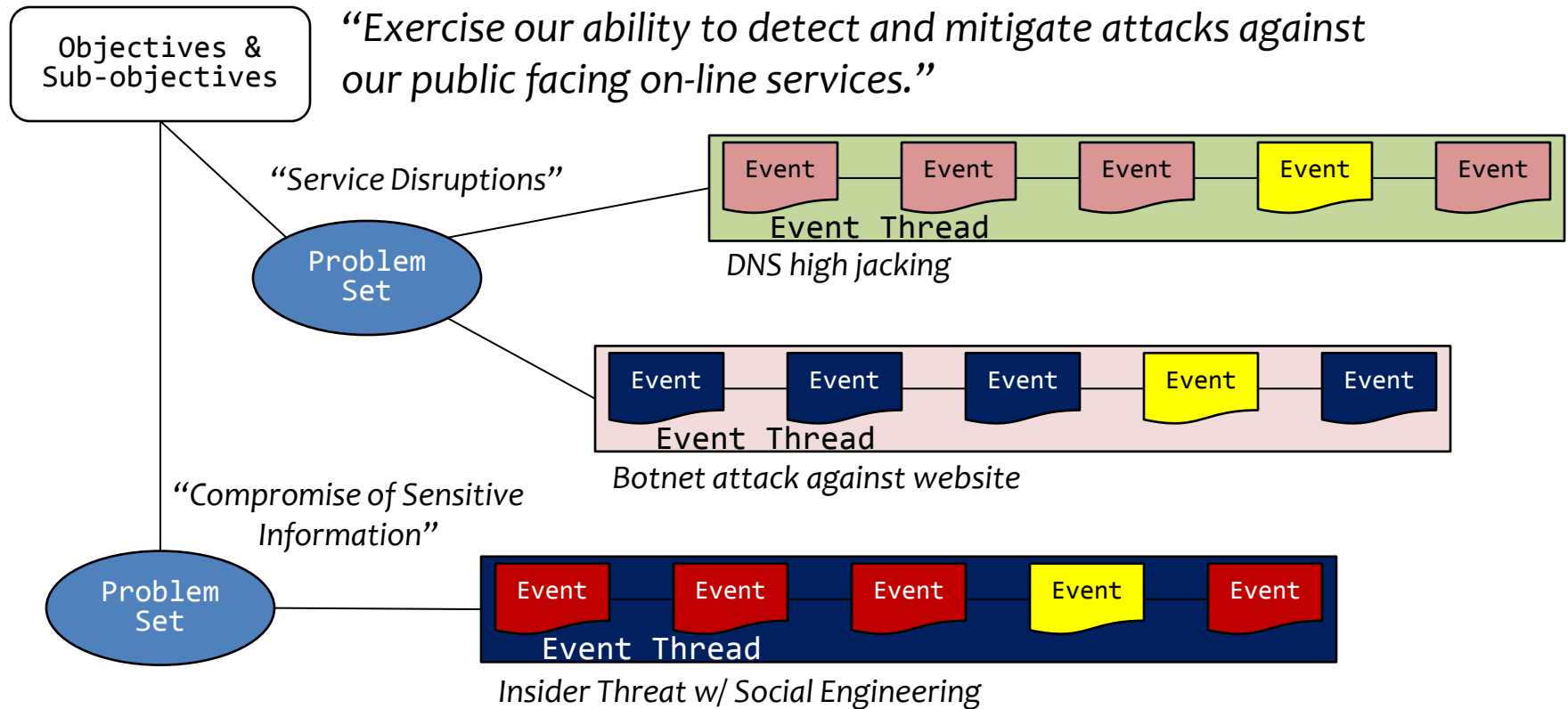
# Scenario Planning (cont.)



## Key Scenario Elements affect:

- ... who you get to participate
- ... what expertise you need for planning
- ... what procedures you focus on for execution

# Organizing the Events



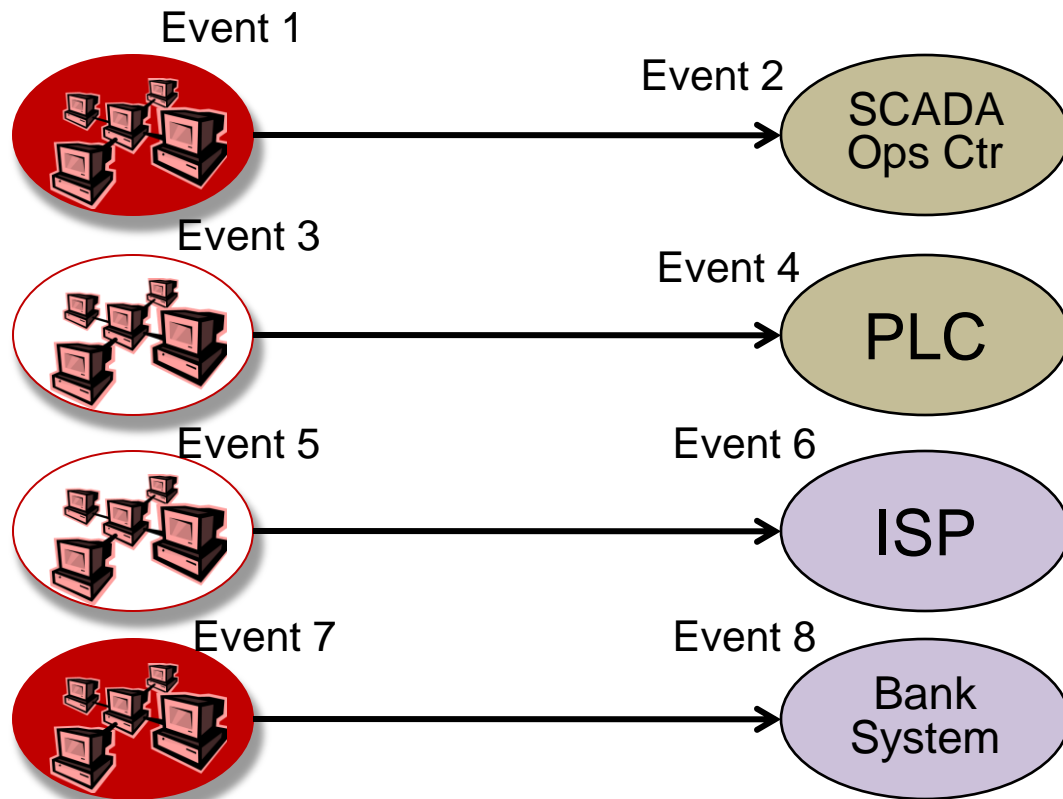
*How does this look in a MSEL?*

# Managing the Complexity

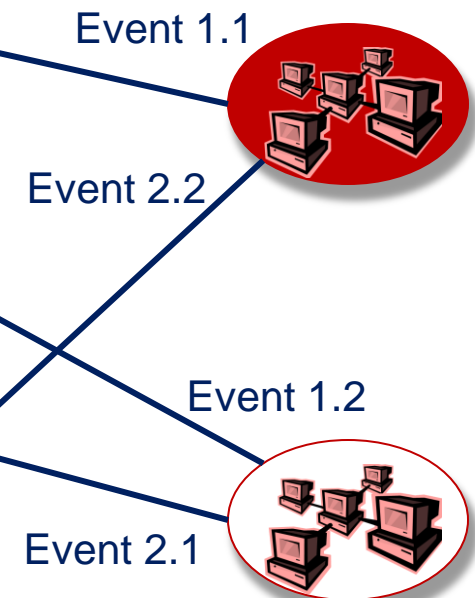
For a TTX ... this might be sufficient

*“Cyber terrorists conducted a large-scale cyber attack that shut down portions of the electric grid and disrupted on-line banking transactions.”*

Traditional MSEL ...



“Enhanced” MSEL ...



# Enhanced MSEL

## HSEEP MSEL

- designated scenario time
- event synopsis
- name of the controller responsible for delivering the inject
- special delivery instructions
- task and objective to be demonstrated
- expected action, intended player, notes

**“Playbooks”**

## Enhancements

- Problem Set
- Event Thread
- **Estimated event end time (duration)**
- Environment configuration actions
- Event instructions
  - Controller instructions
  - Evaluator cues / instructions
  - Aggressor actions / instructions

*Playbooks tailored to location, function, or event thread*

# Scenario Planning Tools ... briefly



*Microsoft® Office,  
Visio, Project*

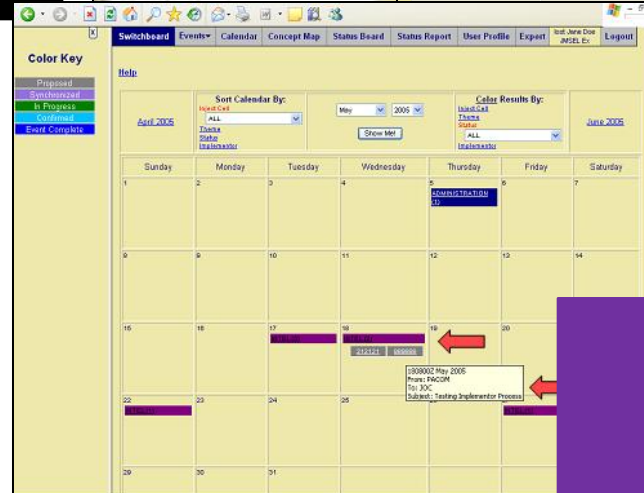
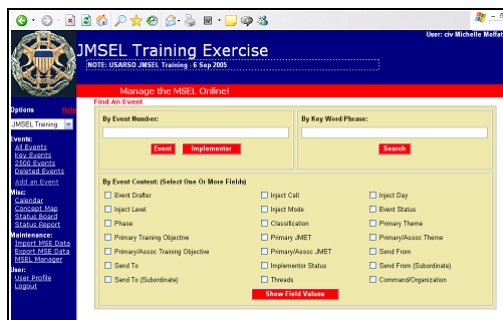
## 1<sup>st</sup> Generation

### National Exercise Master Scenario Events List (NxMSEL)



**MSEL Response Cell Calendar, colored by Status**

Event ID	Event Name	Status	Event Number
20001	20001	Proposed	20001
20002	20002	Proposed	20002
20003	20003	Proposed	20003
20004	20004	Proposed	20004
20005	20005	Proposed	20005
20006	20006	Proposed	20006
20007	20007	Proposed	20007
20008	20008	Proposed	20008
20009	20009	Proposed	20009
20010	20010	Proposed	20010
20011	20011	Proposed	20011
20012	20012	Proposed	20012
20013	20013	Proposed	20013
20014	20014	Proposed	20014
20015	20015	Proposed	20015
20016	20016	Proposed	20016
20017	20017	Proposed	20017
20018	20018	Proposed	20018
20019	20019	Proposed	20019
20020	20020	Proposed	20020
20021	20021	Proposed	20021
20022	20022	Proposed	20022
20023	20023	Proposed	20023
20024	20024	Proposed	20024
20025	20025	Proposed	20025
20026	20026	Proposed	20026
20027	20027	Proposed	20027
20028	20028	Proposed	20028
20029	20029	Proposed	20029
20030	20030	Proposed	20030
20031	20031	Proposed	20031
20032	20032	Proposed	20032
20033	20033	Proposed	20033
20034	20034	Proposed	20034
20035	20035	Proposed	20035
20036	20036	Proposed	20036
20037	20037	Proposed	20037
20038	20038	Proposed	20038
20039	20039	Proposed	20039
20040	20040	Proposed	20040
20041	20041	Proposed	20041
20042	20042	Proposed	20042
20043	20043	Proposed	20043
20044	20044	Proposed	20044
20045	20045	Proposed	20045
20046	20046	Proposed	20046
20047	20047	Proposed	20047
20048	20048	Proposed	20048
20049	20049	Proposed	20049
20050	20050	Proposed	20050
20051	20051	Proposed	20051
20052	20052	Proposed	20052
20053	20053	Proposed	20053
20054	20054	Proposed	20054
20055	20055	Proposed	20055
20056	20056	Proposed	20056
20057	20057	Proposed	20057
20058	20058	Proposed	20058
20059	20059	Proposed	20059
20060	20060	Proposed	20060
20061	20061	Proposed	20061
20062	20062	Proposed	20062
20063	20063	Proposed	20063
20064	20064	Proposed	20064
20065	20065	Proposed	20065
20066	20066	Proposed	20066
20067	20067	Proposed	20067
20068	20068	Proposed	20068
20069	20069	Proposed	20069
20070	20070	Proposed	20070
20071	20071	Proposed	20071
20072	20072	Proposed	20072
20073	20073	Proposed	20073
20074	20074	Proposed	20074
20075	20075	Proposed	20075
20076	20076	Proposed	20076
20077	20077	Proposed	20077
20078	20078	Proposed	20078
20079	20079	Proposed	20079
20080	20080	Proposed	20080
20081	20081	Proposed	20081
20082	20082	Proposed	20082
20083	20083	Proposed	20083
20084	20084	Proposed	20084
20085	20085	Proposed	20085
20086	20086	Proposed	20086
20087	20087	Proposed	20087
20088	20088	Proposed	20088
20089	20089	Proposed	20089
20090	20090	Proposed	20090
20091	20091	Proposed	20091
20092	20092	Proposed	20092
20093	20093	Proposed	20093
20094	20094	Proposed	20094
20095	20095	Proposed	20095
20096	20096	Proposed	20096
20097	20097	Proposed	20097
20098	20098	Proposed	20098
20099	20099	Proposed	20099
20100	20100	Proposed	20100



### Joint Master Scenario Events List (JMSEL)

## 2<sup>nd</sup> Generation



# Scenario Planning Tools ... briefly

## Cyber Scenario Modeling and Reporting Tool (CyberSMART) v1.0

**Switch to Data View**

**Concepts & Objectives Meeting**

Exercise Description

Exercise Objectives (3)

Scenario Ideas

Sectors (7)

Nations (2)

Exercise Venues (5)

**Initial Planning Conference**

Organizations (9)

Exercise Modules (3)

Threat Description

Scenario Summary

Shared Resources (5)

Problem Sets (3)

**Prior to MPC**

Organization Objectives (2)

Critical Electronic Transactions (4)

IT Assets (2)

**Mid-term Planning Conference**

Problem Sets (3)

Story Board

Red Threats (2)

Other Threats (1)

Player Roles (4)

Simcell Players (5)

**Prior to**

Event Threads (17)

Scenario Events (52)

**Final Planning**

Event Review and A

Visualization

Reports and Queries

**User Pr**

User Information

Audit

**Switch to Planning View**

**Exercise Definition**

Description

Modules (3)

Venues (5)

**Objectives**

Objectives (3)

ation Objectives (2)

**Game Space**

(7)

(2)

Resources (5)

tions (9)

Electronic Transactions (4)

ts (2)

Roles (4)

Players (5)

**Events Timeline**

**Exercise: Northern Summer**

Problem Sets: All problem sets

Event Threads: All event threads

Timezone: GMT

Update

Inquiry from tax payer is

State Tax Site phishing

New event

Web Server is compromised

Web Defacement of Flu-web

Web defacement

The email is a forgery Review

Safety DB compromise

Safety records and accident

FN gains access to wireless

6 support machines attack

Timeline: 6hr, 7hr, 8hr, 9hr, 10hr, 11hr, 12hr, 13hr, 14hr, 15hr, 16hr, 17hr

Steps: Sep 16, Sep 17, Sep 18, Sep 19, Sep 20, Sep 21

Scenario: Story Board 5.6.1 - Mozilla Firefox

file Edit View History Bookmarks Tools Help

https://cybersmart.usurf.usu.edu/index.php?id=49f6a0d0061&ur=5\_6\_1

Getting Started Latest Headlines

Scenario: Story Board 5.6.1

ESMT Visualization

**CyberSMART**

**Northern Summer**

cfogle: Exercise

User venue: Control

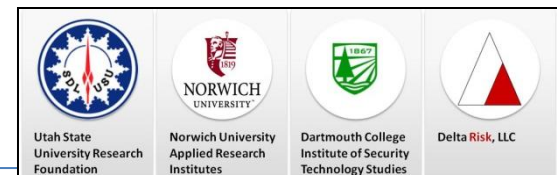
Switch to Data View

Wiki Help

Report a bug

Scenario: Story Board

Problem Sets	Unassigned Modules	Prevention	Response	Background noise, simple uncoordinated failures and attacks	Recovery	Failing efforts to
Transportation Disruptions	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread
Attacks on State Government IT	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread
Disruption of business activities of key manufacturing organizations	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread
Hospital attack	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread
Attacks on energy	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread
Web Based Flu Data	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread
Disruption of Emergency Communications	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread
Big Long Problem Set Name that will Crowd Out Everything	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread	Add Event Thread



Next Generation

---

... after the planning, EXECUTE

# **LIVE-ACTION AGGRESSORS & PLAYING ON THE OPERATIONAL NETWORK**

# Live-action aggressors ... What's in a name?

## Vulnerability Assessment Team

“Dig around, see what you can find, and document the problem – maybe a recommended fix-action, too”

## Red Team

“Dig around, see what you can find, and clearly demonstrate or document the impact”

## Aggressor



“Be the specific adversary – read up on their TTP, get their tools or techniques, and execute a structured battle plan while providing requested stimulus”

**“THREAT EMULATION”**

*... and don't forget skill and maturity*

# Exercising on Operational Networks



*10 missions; only 2 on operational network  
... but it changed with demonstrated capability*

- ✓ “Low and Slow” probing, scanning, and enumeration
- ✓ Denial of Service (systems)
- ✓ Rogue systems & access points
- ✓ Phishing – email and web
- ✓ Zero-day
- ✓ Host compromise (virus/malware, hacked)
- ✓ Data exfiltration
- ✗ Worm attack
- ✗ Denial of Service (bandwidth)
- ✗ Widespread Botnet attack (target or zombie)

# Considerations for Exercising on Ops Networks

---

- IP / host deconfliction tables; map aggressor exercise IP space to “real-world”
- Use known vulnerabilities; unpatch or misconfigure the system for execution
  - Block external access at the firewall; restrict by IP address
- Use tools to monitor traffic to exercise systems
- Leave system disconnected from the network until needed within the exercise
- Set an administrator password; use an access authentication and traffic encryption
- Use Media Access Control (MAC) address filtering and limit Dynamic Host Configuration Protocol (DHCP) lease

---

... for those things you just can't do on the network

# **SIMULATORS AND RANGES**

# Simulators and ranges

---

- BLACK DEMON ranges
  - Fielded net defense tools, separate network that looked like Air Force NOSCs and NCCs; Simple traffic generation, not stateful
- Simulator Training Exercise (SIMTEX)
  - Formal program that evolved from BLACK DEMON; fixed-architecture duplicated AF net defense apparatus
  - Rapid improvements in traffic generation and realistic attack signatures
  - Used in BLACK DEMONs and BULWARK DEFENDER

# Simulators and ranges

- Exercise Network (XNET)
  - Developed by Software Engineering Institute at Carnegie Mellon University
  - Virtual machine technology and “push-button” deployment of multiple, simultaneous exercise environments; customized scenarios
  - Centralized, isolated, and dedicated exercise environment significantly reduces setup and configuration time
  - Easily customized Threat scenarios and realistic threat model
    - Timeline and Event Library, Drag and Drop attacks/anomalies
  - Automated data collection
    - Real-time readiness metrics
  - Allows for experienced cadre to enable local crew training

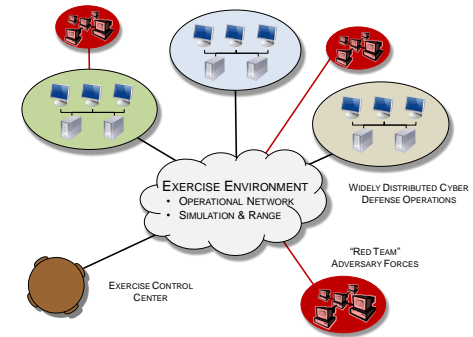


# Simulators and ranges

- Cyberoperations Enhanced Network & Training Simulators (CENTS™)
  - Developed by EADS North America, Defense Security and Systems Solutions, Inc. (DS3)
  - Emulates a desired operational network architecture & uses existing Wide Area Network transport
  - Virtual Machine Technology
    - Network sensor systems, switches, routers, firewalls, servers, domain controllers, email, and other various network services normally found in most computer network architectures
  - Vulnerabilities can be built in to the simulator to provide the crew exposure
  - Operated both as a single system or a network of systems connected by a secure Virtual Private Network (VPN)
    - Cybersecurity Network Training Simulator (CYNTRS®) for crew training
    - Hands-On-Training Simulator (HOTSIM®) for classroom training

# Final Thoughts on Raising the Bar...

- Community dialogue on advanced cyber exercise methods and practices
  - Simulator and range technologies
  - Planning methodologies and tools
  - Cyber exercises and HSEEP
- Courses for cyber exercise planning and execution
  - Indoctrination for all-hazards practitioners
  - Threat emulation and skills training, certification
- Scenario templates
  - Lessons learned, central repository of best practices



# Contact

---

- Chris Fogle, CISSP  
Delta Risk, LLC  
[cfogle@delta-risk.net](mailto:cfogle@delta-risk.net)



- ***Strategic Consulting & Policy Development***
- ***Operational Concept Development***
- ***Security Program Assessment***
- ***Advising technology development***
- ***Cyber Exercises - Planning & Execution***
- ***Training Programs & Courseware***
- ***Expert Witness Services***